

NAVAL WAR COLLEGE
Newport, R.I.

EXECUTING JOINT INFORMATION OPERATIONS: WHERE DO WE GO AFTER KOSOVO?

BY

MAJ SCOT D. MACKENZIE, USA

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

5 February 2001

DISTRIBUTION STATEMENT A

Approved for Public Release
Distribution Unlimited

Signature:

20010510 179

REPORT DOCUMENTATION PAGE

| | | | |
|--|-------------------|---|------------|
| 1. Report Security Classification: UNCLASSIFIED | | | |
| 2. Security Classification Authority: | | | |
| 3. Declassification/Downgrading Schedule: | | | |
| 4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. | | | |
| 5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| 6. Office Symbol: C | | 7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207 | |
| 8. Title (Include Security Classification): Executing Joint Information Operations: Where Do We Go After Kosovo? (Unclassified) | | | |
| 9. Personal Authors: Scot D. MacKenzie, Major, USA | | | |
| 10. Type of Report: FINAL | | 11. Date of Report: 5 FEB 01 | |
| 12. Page Count: 21 | | 12A Paper Advisor (if any): | |
| 13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | | | |
| 14. Ten key words that relate to your paper: Information Superiority, Operations, Doctrine, Strategy, IO Cell, Kosovo, Operation Allied Force | | | |
| 15. Abstract: Operation Allied Force, the NATO air operation in Kosovo, was the first major operation where Information Operations (IO) was formally implemented, albeit with mixed results. Like many other aspects of this historic operation, IO affects were prosecuted in piecemeal fashion and far too late to be effective. Alliance problems aside, the joint warfighting team raised many concerns for how IO affects are integrated into joint and combined operations. While the IO report card is bleak, it is important to examine what went wrong and take steps to improve IO during future joint operations. We have far to go as a joint community until we see the full strategic benefit of IO, which doctrine suggests is to "affect adversary or potential adversary decision makers to the degree that they will cease actions that threaten U.S. national security interests." ¹ This paper proposes taking two concrete steps to elevate the importance of information by recognizing IO as a unique operational planning and execution function. . At the core of my proposal is forming a permanent IO cell, properly staffed, and led by senior leadership. This cell will develop the precursor for successfully executing IO: a theatre-wide IO strategy that is fully coordinated with all non-DOD agencies in an AOR. My thesis is generated from the IO lessons from Kosovo, namely: 1) Make sure people know what IO is; 2) Start IO very early in planning; 3) Have a adequately staffed IO cell headed by senior staff officer; 4) Have an IO strategy that is implemented during peace <i>and</i> crisis. Kosovo bears out one important point: Joint IO is not ready for prime time. | | | |
| 16. Distribution / Availability of Abstract: | Unclassified X | Same As Rpt | DTIC Users |
| 17. Abstract Security Classification: UNCLASSIFIED | | | |
| 18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| 19. Telephone: 841-6461 | | 20. Office Symbol: C | |

Introduction:

Operation Allied Force (OAF), the NATO air operation in Kosovo, was the most recent operation in which Information Operations (IO) was formally implemented, albeit with mixed results. To clarify, IO is "actions taken to affect adversary information and information systems while defending one's own information and information systems."¹ Like many other aspects of this historic operation, IO effects were prosecuted in piecemeal fashion and far too late to be effective. Alliance problems aside, the joint task force raised many concerns regarding how IO effects are integrated into joint and multinational operations. While the IO report card is checkered, it is important to examine what went wrong and take steps to improve IO in the future. I believe we have far to go until we see the full strategic benefit of IO, which doctrine suggests is to "affect adversary or potential adversary decision makers to the degree that they will cease actions that threaten U.S. national security interests."²

My analysis uses current joint doctrine and the IO lessons from Kosovo to examine how we can improve IO execution in the *next* major joint operation, recognizing that these proposals are not the panacea, only an incremental step toward the larger IO issues that must be resolved in the coming decade. I contend that our problems in Kosovo stem from the fact that IO is still new and quite complex, as is evidenced by current doctrine. We must fix two areas now, the IO cell organization and IO strategy development, in order to improve from Kosovo. I base both recommendations on the premise that information, if applied properly, can be a unique operational function capable of compelling our adversaries to do our will. This idea, although very prevalent in our current military lexicon, is still years from being completely realized due to a basic

lack of knowledge across the services. What is needed is a paradigm shift: Instead of engaging our adversaries with only kinetic means, we can theoretically increase our effectiveness with non-kinetic efforts such as IO. How well we attack this challenge, however, will be directly proportional to the value our regional CINC's place on information.

Thesis: My Two Proposals.

The major IO shortfalls from Kosovo were: 1) Lack of knowledge and perceived importance for IO; 2) IO started too late in the operation to be effective; 3) the IO cell had no plan to build from; 4) Lack of access (compartmented vs. non-compartmented) between cell members; and 5) the IO Cell was physically separated in two locations.³ My focus is to identify how can we improve in these areas.

My first proposal is to modify the “one size fits all” IO cell listed in Joint Publication 3-13, “Joint Doctrine for Information Operations,” and divide it into three distinct groups. I believe the IO Cell, which plans and executes all IO functions for a CINC, is too large to resource and operate. Moreover, the CINC does not get extra people to man the cell, which means a large number of people have to buy in to its importance in order to *properly* staff the cell. Who do you really need? My proposal is to maintain a smaller, permanent, core cell of functions that grows as required during transition from peace to crisis. Current joint doctrine is a mark on the wall that, in the case of the IO cell, has been quickly overcome by real world experiences. Establishing a smaller IO cell seems logical in view of the manning and training requirements inherent with its organization.

Core cell members should include J2, J3, J6, and Special Technical Operations (STO) representatives, and the senior Psychological Operations (PSYOP) staff officer. These are your "must have" players since they represent the foundation for all IO: intelligence, communications, STO, targeting, and PSYOP. The cell should be headed by a senior officer, which I propose is the deputy J3 (DJ3). If you want to give IO credibility, put a senior officer in charge who is in a position to properly integrate IO effects. Moreover, the core cell should be part of the Deployable JTF Augmentation Cell (DJTFAC) to ensure IO is involved in the early part of a crisis. Finally, organize an IO steering committee headed by the Deputy CINC (DCINC) to set IO policy and check progress periodically. This senior level focus is necessary to implementing a strategy that requires interagency involvement.

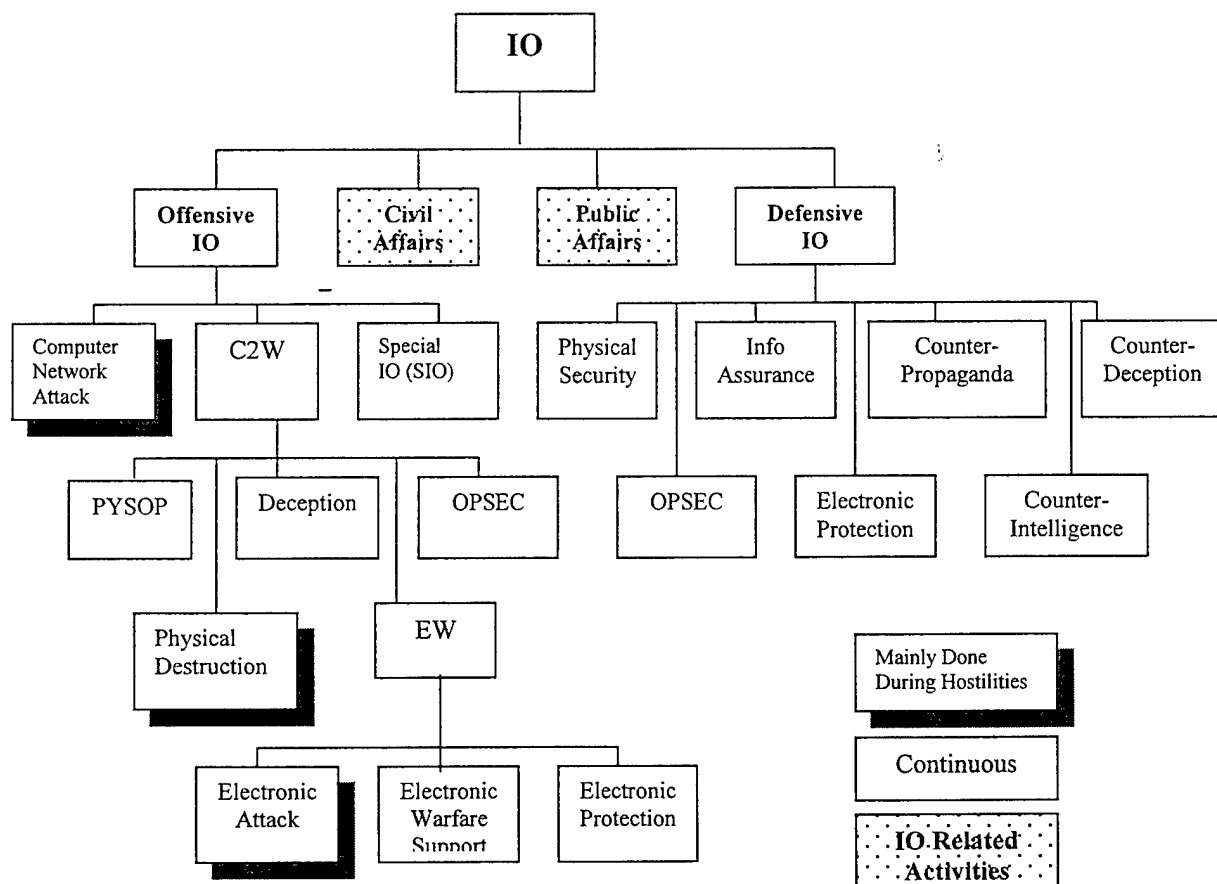
My second recommendation addresses another shortfall from OAF: development of a theater IO strategy. JP 3-13 states that strategy is vital to implementing IO but only broadly covers how this could be done. My analysis addresses how the IO cell could begin to craft a strategy that is *active* in peacetime and prepared to transition to crisis. Formulating a strategy is not simply a military function, but relies heavily on non-military agencies whose influence in an AOR is crucial to promoting and shaping regional stability. Doctrine states that "IO can make an important contribution to diffusing crises" and "IO at the national-strategic and theater-strategic levels requires close coordination among numerous elements of the USG (US government), to include the DOD."⁴ Implicit in both statements is the need to have an active strategy *before* a crisis occurs.

Peacetime engagement, and certainly IO, is about perception management, or getting your adversary to think and act the way you want. To do this we need better coordination between a CINC and the non-DOD "information players" in the region, i.e. Department of State (DOS), Central Intelligence Agency (CIA), Department of Commerce (DOC), and other key government agencies active in an AOR. These are the groups most capable of shaping perceptions in an AOR through words or deeds, and if their efforts are uncoordinated, they can actually work against each other.

The premise to my vision of an IO strategy is developing information objectives (messages/themes) for an AOR, and then deciding ways to use the military and non-military tools available to identify targets and apply our effects. I consider this action "Peacetime IO Targeting." The target could be an adversary leader, populace, or opposition group, and the weapon is information. In my opinion, offensive IO *is* targeting, but we must continually target IO effects based on the specific information objectives established. Peacetime targeting constitutes an active strategy versus having a plan on the shelf for use only in crisis. Proper IO execution requires developing target sets for peacetime and crisis, with the latter complementing the peacetime plan. In peacetime, you engage with subtle, and sometimes, covert means. During a crisis, IO expands its targeting to apply many of the offensive forms of IO (EW, physical attack, Computer Network attack) while maintaining defensive measures to ensure our ability to act. The payoff is a smoother transition in the early stages of crisis when IO is essential to setting conditions in the minds of our adversaries.

What is IO, really?

It is important to understand all the activities that constitute IO. Information Operations encompasses four primary capabilities; 1) Perception Management, through the use of PSYOPS, Deception, Civil Affairs, and possibly even Public Affairs; 2) Physical Effects, which include EW, physical destruction, Special Technical Operations, and the emerging capability of computer network attack (CNA); 3) Information Protection, which includes physical security, information assurance, OPSEC, and electronic protection; and 4) Defensive Counter-Information, which includes counter-propaganda, counter intelligence, and counter-deception. See diagram below.



*Taken from the Joint IO Planning Handbook, 2d Draft, JCIWS, January 2000

So the question remains: what does it really mean? It means IO is a comprehensive program for targeting kinetic (physical effects) and non-kinetic means (perception management/counter-information) against adversary decision makers while protecting yourself against the same. IO in its simplest form is targeting, only the targets, and sometimes the weapons used, are different. IO is not a stovepipe effect (one bomb, one target) but a mutually supporting set of *activities* that, if integrated properly, “may have greatest impact as a deterrent in peace and during the initial stages of a crisis.”⁵ For this reason, IO is something that cannot be cobbled together quickly in a crisis if it is going to produce decisive effects. It relies heavily on C4I systems and intelligence to provide the foundation for planning and execution, with the peacetime objective being to shape adversary perceptions (deter) and in crisis, to serve as a key player in the overall targeting process. A review of our most recent effort in applying those concepts, however, proves there is a major gap between concept and reality.

What Went Wrong in Kosovo?

It is important to review the results of OAF to see where the implementation challenges lie. Simply put, IO doctrine briefs much better than it works. Some basic questions remain after this operation; can we execute our doctrine as written or do we need to revise it? Is IO too broad a concept to translate into measurable affects? Can IO be seen as helping a CINC reach his objectives? All are worthy to consider as we examine the OAF Case Study.

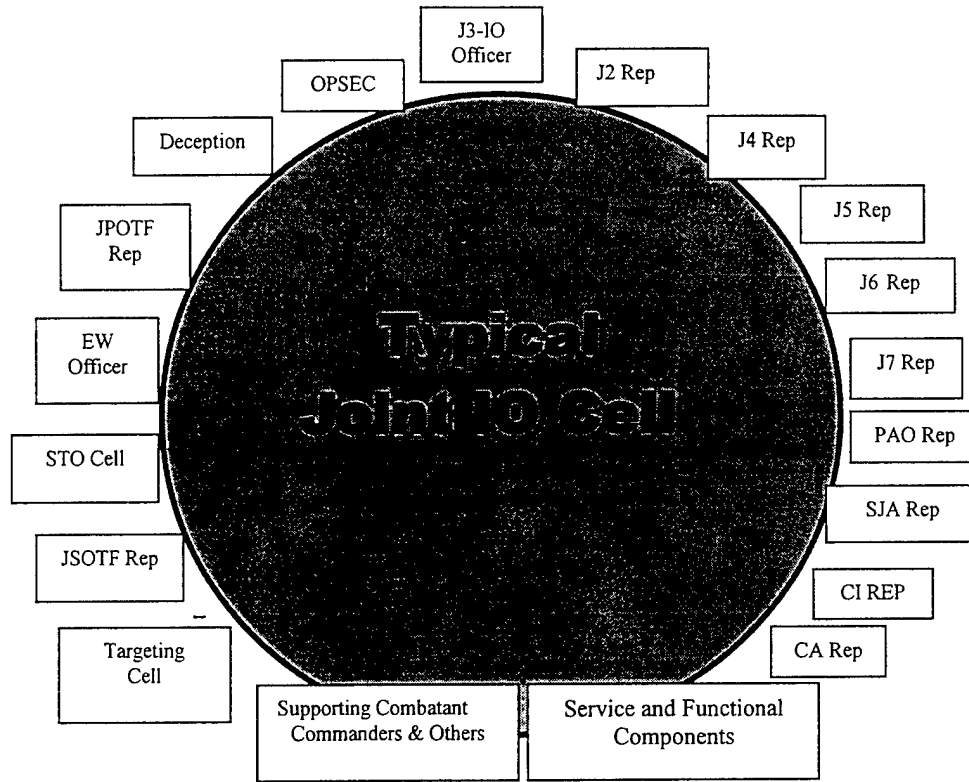
The primary problem in OAF was lack of friendly knowledge about IO.⁶ Instead of spending time coordinating effects, the IO cell chief had to brief key staff members on what IO was and how it could be incorporated in targeting. This "sales pitch" strategy

belies the fact that IO is still seen as a peripheral enabler to warfighting that can easily be overlooked. To add to that perception, IO was begun nearly 30 days after the bombing started.⁷ This hurt its effectiveness and proved that significant advanced planning is required to realize measurable effects. The fact remains that many still see IO as a stovepipe effect that can be easily added to an operation, not a “family of effects” that must be integrated into an operational plan.

The organization of the IO cell was another problem. Whether intended or not, the JTF Commander sent a clear message about the importance of IO when he appointed a Navy O-4 cryptologist as cell chief. Moreover, there was no IO plan to work from and the cell essentially made their plans up as they went.⁸ On any joint staff, individual credibility is largely based on position and rank, of which this cell chief had neither. An example of rank mismatch was the Joint PSYOP Task Force (JPOTF) Commander, who was an Army O-6 and a key player in IO planning and execution. At a minimum, the cell chief should be of equal rank to every member of the IO team or you have the potential for serious conflicts. Instead of key staff sections sending representatives to work in the IO cell, the opposite was the case. Additionally, many of the IO cell members were actually subsumed by their parent staff sections to work competing requirements unrelated to IO.⁹ Lack of rank, experience, and position proved a debilitating factor in coordinating activities, to include planning meetings with other JTF staff members. Moreover, the staff was split between two locations, which made coordination of cell activities more difficult. These constant challenges undercut the overall integration effort and proved that you cannot execute IO under these conditions.

Doctrines' IO Cell: "Bigger is Better" Approach has Problems.

Why did the OAF IO cell have these problems? In part it points to the difficulty in organizing the cell in accordance with doctrine, which should be modified. But before getting to my proposed changes, I want to examine some of the limitations in carrying out JP 3-13's version of the typical IO cell, which is shown below.



My first thought after seeing this cell was "wishful thinking." It seems apparent that when JP 3-13 was written, doctrine writers did not want to leave any capability out. The result is a cell that is simply too large to be effective, especially since Unified Commands or JTFs are not resourced to staff it. Trying to merge this many functions into one cell, based on our collective knowledge of implementing IO, seems overly ambitious. This leaves manning to the good graces of many different sections/components, which probably means getting less than adequate people to fill

some slots. Such a large cell puts a tremendous burden on the IO officer to conduct planning and coordination, and almost mandates being co-located to be effective, which was a problem in OAF. Additionally, the training burden (specialized schooling) for such a staff is also immense and one that most CINC's would not resource.

Overall, the limitations in a large cell far outweigh the likelihood for success as evidenced by the staffing, planning, and training challenges. So who are the most important players? One cannot tell when reviewing JP 3-13. This is why it is important to narrow the field to simplify planning and execution. Therefore, we should identify the key personnel required at all times, and what players could be added as required during a crisis. This step follows my incremental approach philosophy for improving joint IO.

My IO Cell: Smaller is Smarter.

To attack the issue of organization, some questions should initially be answered. Whom do you really need in an IO cell? How many people can the CINC adequately resource and *train*? Who should lead the cell? JP 3-13 states that the IO officer will normally be designated by the J3, but does not offer any recommendations. I submit that if you choose the wrong officer, someone of junior rank who is unfamiliar with the OPLAN, you will certainly have problems. Operations (J3) personnel are the true synchronizers for any operation, but not any J3 representative will do. Your cell chief must have clout.

My recommendation for IO cell chief is the deputy J3 (DJ3). This is the CINC's number two operations officer and one who is in a unique position to fill this slot. The DJ3 is very familiar with the operational plans of a Unified Command or JTF and would understand where IO could be integrated. They will normally be senior, O-6 or flag

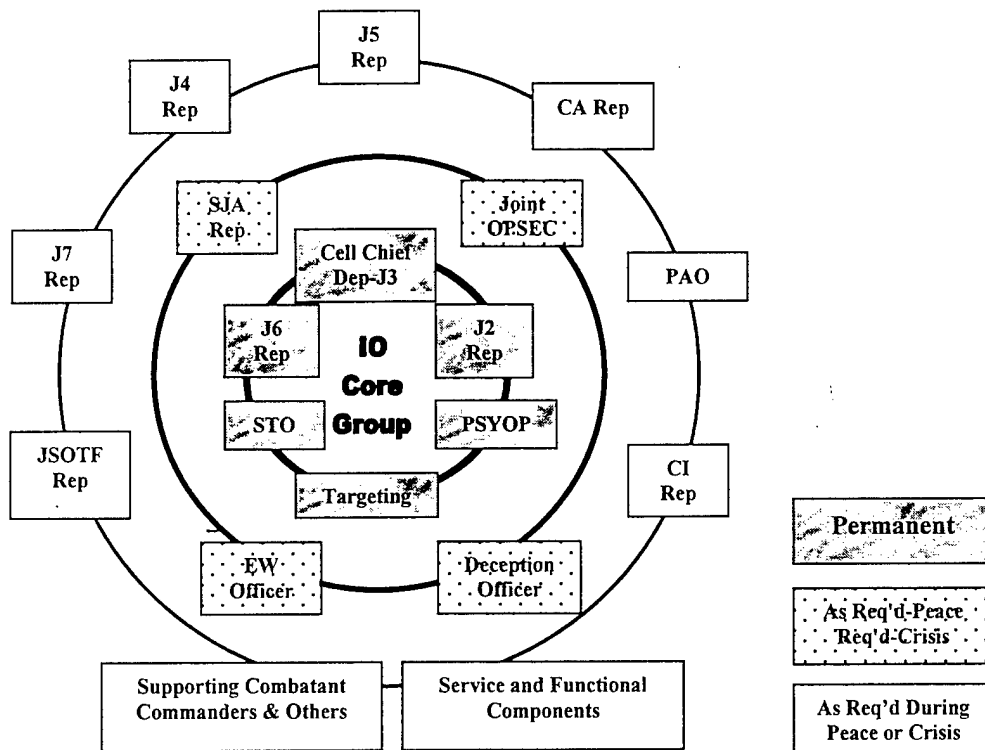
officer, and in a position to exert influence over the primary staff members assigned to it. This officer gives the cell credibility and visibility, and ensures IO a "seat at the table" when integrating their priorities during the joint targeting process.

An argument can be made against this choice because this takes the DJ3 away from his traditional duties, but it can also be made for almost any staff representative assigned to the IO cell. This gets back to how important the IO cell is to the CINC. If IO is a priority, he will resource it with the right people. If the goal, however, is to treat it as a secondary effort, staffing will follow accordingly. Choosing the DJ3 will set the tone for staffing the entire cell.

The next task is to identify what capabilities would be required to do IO planning in both peace and crisis. I have divided the cell into three rings, each representing various capabilities, and have not deleted any slots from JP 3-13. The absolute essentials are the IO core group, which should be permanent members. This group includes a Targeting officer (J2 or J3 rep), representatives from J2, J6 and STO, and a PSYOP Officer. I chose these personnel because they represent the foundation for all IO planning, and each will serve as valuable liaisons in their particular fields.

The J2 officer coordinates collection requirements and analytical support for compartmented and non-compartmented information, and will serve as a liaison to agencies such as the CIA and DIA. The J6 representative facilitates information assurance coordination; ensures the targeting officer minimizes risk to friendly C2 capabilities, and is a liaison to the JCCC and DISA. The PSYOP officer is the direct link to the PSYOP TF Battalion Commander and other PSYOP cells in the theater, and is very familiar with the Overt Peacetime PSYOP Program (OP3), which is an active

Psychological Operations program in the AOR. The STO representative on the CINC's staff is vital to coordinate support from the Joint Warfare Analysis Center (JWAC), Joint Spectrum Center (JSC), and compartmented capabilities. The final member is a targeting officer, who will work with all members of the cell to develop peacetime and crisis IO target lists, as well as serve as the cell's representative to the Joint Targeting Coordination Board. See the revised IO cell diagram below.



Second ring members include a Joint OPSEC officer, Electronic Warfare (EW) officer, Staff Judge Advocate (SJA), and Military Deception Officer (MILDEC). I consider these four personnel "As required during Peace, Required in Crisis." Depending on the complexity or aggressiveness of the peacetime IO strategy, the OPSEC, SJA, and MILDEC may be required at all times, while the EW officer is normally only used during a crisis. Expanding the core group is a decision that must be made by the IO cell chief, in

coordination with effected staff sections. Together these 10 positions comprise the minimum required elements of an IO cell during a crisis, with each representing the majority of offensive and defensive IO expertise.

The remaining representatives in the third ring are important, but will be required based on the mission. Some have made cases that Civil Affairs and Pubic Affairs should be permanent members, but I argue otherwise. Both functions are listed as being "IO related" activities in the Joint IO Planning Handbook, soon to be published by the Joint Command, Control, and Information Warfare School. Nearly all CA units are in the Reserve Component and there is not even a CA staff officer on a CINC's staff, which would make peacetime planning very difficult to accomplish. I do not dispute the role of Public Affairs in an IO strategy, but there are fundamental conflicts between their role as truth tellers and the IO role of using PA as a tool to manipulate or deceive our adversaries. The remaining representatives will be needed at times, but I cannot make strong case for them as permanent members.

A key point: access for all core group members must be unlimited to remove the issues of dealing with compartmented capabilities that reside in the military and outside agencies. One of the IO problems during OAF involved access, which is not surprising considering what capabilities were employed. If the IO cell is going to prosecute the full complement of capabilities in a theater, core cell members must have full knowledge to the extent necessary to plan and execute IO activities. This means that cell members cannot be cast-offs provided to meet the cell manning requirement; rather they need to be very capable in their fields and properly cleared to handle the most sensitive materials. Unlimited access may be difficult to attain, especially when dealing with outside

agencies, but is worth pursuing to allow the IO cell maximum opportunity to coordinate their activities.

The final element to assist the core group involves forming an IO steering committee,¹⁰ which would provide direction and policy guidance. Once again, the level of importance placed on IO will drive the selection of the OIC and steering group members. I propose selecting the Deputy CINC (DCINC) as OIC. Members of the steering group could include the primary staff officers (J2-J7), POLAD, other agency representatives as desired, and properly cleared embassy representatives for specific embassies in the AOR.

The steering group could meet twice a year and serve a dual purpose. This group could provide senior level focus and, by virtue of their involvement, keep the CINC's primary staff members and key players engaged in IO planning and execution. Also, if the IO staff is working with outside agencies in peacetime IO targeting, senior leadership might be important to facilitate this coordination. The IO cell could update the steering group on current and future activities while better synchronizing IO efforts across the staff. Recall that IO knowledge was very limited during OAF, which makes this steering group a natural mechanism to improve the knowledge gap.

How do we get the IO cell engaged early during a crisis? I propose that the core cell be available to deploy as part of the DJTFAC. It makes sense to send the people who have been involved in peacetime IO planning/targeting and have detailed knowledge of the crisis targeting plan. As in any operation, they could be redeployed if the JTF brings adequate members to execute IO during the crisis, but the permanent cell would be there to ensure IO effects were commenced properly.

Developing an IO Strategy.

Once established, developing an IO strategy becomes job one for the IO core group so that we do not repeat what happened in OAF. Why *was* IO such an afterthought? Much of the literature indicates that IO, like many other aspects of the operation, was ill planned because of the pervading belief that Milosevic would capitulate after being struck with limited air strikes. The Kosovo report to Congress stated that, "Planning focused on air strikes and diplomacy as the primary tools to achieve U.S. and NATO objectives. As it became clear that Milosevic intended to outlast the alliance, more attention was paid to other ways of bringing pressure to bear, including economic sanctions and information operations. While ultimately these instruments were put to use with good effect, more advanced planning might have made them more effective at an earlier date." ¹¹ This statement highlights the need to start IO early in the operation, but we must go farther than that. IO planning needs to occur *before* a crisis. Moreover, many of the IO activities listed on page 5 are "continuous", which implies implementation during peacetime as well as crisis. The only way I see this happening is to develop and implement a peacetime strategy.

In drafting such a strategy, one must recognize information as the key enabler for a CINC to shape the strategic environment. Peacetime engagement is designed to bolster regional relationships, promote stability, maintain readiness, and deter our adversaries. While military means are a portion of the tools to carry out a theater engagement strategy, non-military players also shape an environment, such as the Departments of State, Transportation, and Commerce, as well as the CIA and NSA. These groups and others comprise the information players in an AOR.

The National Military Strategy states “Deterrence is the military’s most important contribution to the shaping element of the President’s strategy.”¹² While I do not argue this point, it is clear that the capabilities of our forces, and more importantly, the will to use them decisively, are not always conveyed properly to an adversary. History offers examples of how misperceptions formed from poorly contrived messages, whether from actions or words, can lead to conflict. Recent examples include then U.S. Ambassador to Iraq April Glaspie’s remarks to Saddam Hussein in April 1990, in which she inadvertently portrayed the US as disinterested in Iraq’s disputes with Kuwait, and President Clinton’s statement that we would not use ground forces in Kosovo. These failures to coordinate information objectives undercut the military by conveying the wrong message to an adversary. It seems ironic that while the USG recognizes information as an element of national power it is unclear if we know how to use it to its fullest deterrent value.

An IO strategy is vital to focus the use of information to achieve an objective, which ultimately means to shape perceptions and deter aggression. The USG, namely members of the in-country teams, have a large part in conveying the deterrent messages our CINC’s need to project. To do this will require a significant amount of interagency coordination, but where do we begin?

I propose engaging the non-military players of an AOR to work closely with military planners to coordinate specific *information objectives*, and from these we can build peacetime and crisis IO target lists. What and who are we trying to target? If an adversary leader, what message are we trying to convey? If an opposition group, what activities can be coordinated between the CINC and the various agencies that might be

involved (CIA, DOS, NSA)? What means have we selected (military or non-military), and if in a conflict, lethal or non-lethal means? Are we publicly or covertly targeting, or both? Regardless of our focus, the information objectives must be targeted consistently to avoid sending mixed signals, although I realize the amount of interagency coordination required to do this may be difficult to achieve. Some agencies may not want to divulge their activities, which gets back to the issue of access. This hurdle, however, should not stop an IO cell from attempting to coordinate the activities in the AOR. This might mean that theater engagement plans could be merged with DOS Mission Performance Plans to assure coordination between CINC's and DOS officials. This type of coordination would raise awareness between military and civilian officials about the kinds of activities occurring in a region and would foster greater ties between these organizations and others.

How might peacetime targeting be accomplished? While I admit that my vision is limited based on limited knowledge of our government's capabilities, I offer this example. The leader of country *X* has been identified as the prime target in a peacetime IO targeting list. Using intelligence available between various agencies, we are able to build a credible list of the major military and civilian supporters in his country. These people could be targeted, possibly using email, telephonically, or through third parties, that "an unknown party" has critical information on their family, bank accounts, daily whereabouts, or possibly negative information about their leader. This information could be used to begin organizing support against their leader. Concurrently through other channels, messages from an Ambassador would further amplify our position that we disapprove of the adversary leader and his government. Further activities might include a

regularly scheduled military exercise in which EW assets were used to monitor tactical traffic to gather additional intelligence about their military capability. Combined, these, and other activities could be part of a targeting plan. While uncertain about what a plan would consist of, one thing is clear: we should not have to wait for a crisis to commence to begin action. If a crisis occurs, we would actually increase our activities by employing more offensive IO capabilities, to include physical effects.

How would we begin to coordinate information themes for an AOR? Fortunately for the IO planner, an interagency group already exists to begin this process. Because of PDD 68 (30 Apr 99), the USG recently established the International Public Information (IPI) System, which is designed to “influence foreign audiences in support of US foreign policy and to counteract propaganda by enemies of the US.”¹³ Composed of top officials from Defense, State, Justice, Commerce, Treasury, CIA, and FBI, the primary objective of IPI is to “synchronize the informational objectives, themes, and messages that will be projected overseas.”¹⁴ The core group is chartered by the Under Secretary for Public Diplomacy and Public Affairs at the State Department. The IPI charter is not designed to mislead foreign audiences and that information programs must be truthful. Although this is different than my concept of peacetime IO targeting, it is still a resource to help synchronize the information objectives that have already been coordinated by the IPI.

The products of the IO strategy are two target lists; peace and crisis. While I submit that the peacetime program is much more difficult to execute than a crisis plan, it is important to consider what actions can be done in peacetime to promote a deterrence message other than the conventional military activities such as exercises and security assistance. If we spend the time now to devise target sets for both peace and crisis,

ultimately we will be able to transition between the two much better than was done in OAF.

Recommendations:

I believe the key to making substantive improvements from Kosovo lie in the two focus areas presented in this paper. A permanent IO cell should be formed, but as I've shown, it does not have to include every function in peacetime to be an effective planning cell. It must, however, be properly resourced with six members presented as the core IO group. It is realistic to believe that a CINC could organize and train such a cell with oversight provided by the IO steering group. This step would further elevate the importance of the IO cell by giving it direct access to the DCINC and principle staff members, to include key agency representatives.

Developing an IO strategy is certainly a tougher task, but one that can be done. First it takes vision and then outreach to the information players in the AOR. I can see no better way to devise an *active* peacetime strategy than by coordinating an IO target list based on the information objectives of the CINC, Ambassadors, and other agencies in his AOR. I realize that we are treading on new ground and the path to this thing called Information Superiority is not clear. But the tools of IO, as well as the information players, are readily apparent. Certainly we can chart a direction based on these two things.

The fundamental IO challenge is getting your hands around what it is and its place in joint operations. People have preconceived notions, call it "kinetic thinking," about what warfighting entails and it is difficult to change these beliefs. Advances in weapons technology may stifle new approaches to applying power and limit our effectiveness

against the emerging threats of the next century. The problem is that our adversaries are not the predictable enemies of old, which dictates we adopt new and more effective ways to deter. As retired LTG Short, OAF JFACC, said in a recent discussion, “we need to find a way to better integrate the kinetic and non-kinetic means to achieve our objectives.”¹⁵ No longer can we simply use a one-sided approach to applying military power, as was evidenced during the Kosovo mission. We wanted Milosevic to act a certain way and considered only one means to achieve that objective. Our threats today, many of which are asymmetric, have called us to rethink our tools of deterrence and the ways we influence our adversaries. While we may not find the solutions for some time but it is important to take incremental steps to improve our execution of IO in an effort to use information as a new force multiplier.

Notes

¹ US Joint Chiefs of Staff, Joint Doctrine for Information Operations, (Joint Pub 3-13), Washington DC, 9 October 1998, page vii.

² US Joint Chiefs of Staff, Joint Pub 3-13, pg. 1-3

³ LCDR Connie Frizzel, OAF IO Cell Chief, Telephone conversations, 24 Dec 00 and 31 Dec 00. These lessons were gleaned after discussing the major problems she had in leading the IO cell during OAF.

⁴ US Joint Chiefs of Staff, Joint Pub 3-13, page I-4

⁵ US Joint Chiefs of Staff, Joint Pub 3-13, pg. 1-3

⁶ LCDR Connie Frizzel, OAF IO Cell Chief, Telephone conversation, 24 Dec 00

⁷ LCDR Connie Frizzel, OAF IO Cell Chief, Telephone conversation, 31 Dec 00

⁸ LCDR Connie Frizzel, OAF IO Cell Chief, Telephone conversation, 24 Dec 00

⁹ LCDR Connie Frizzel, OAF IO Cell Chief, Telephone conversation, 31 Dec 00

¹⁰ LTC Zachary Hubbard, Instructor, Joint Forces Staff College, Telephone Conversation, Jan. 2000

¹¹ Report to Congress, Operation Allied Force After Action Report, January 2000, pg. 15

¹² National Military Strategy, Shape, Respond, Prepare Now: A Military Strategy for a New Era, 1997, Pg. 14

¹³ Presidential Decision Directive 68, International Public Information (IPI), www.fas.org/irp/offdocs/pdd/pdd-68.htm,

¹⁴ PDD 68, International Public Information Sheet

¹⁵ LTG(R) Short, former OAF JFACC, personal interview, 14 January 2001.